Les blockchains

Poullet, Yves; Delforge, Antoine

Published in:
Les blockchains et les smart contracts à l'épreuve du droit

Publication date:
2020

Document Version
le PDF de l'éditeur

Les blockchains : un défi et/ou un outil pour le RGPD ?

Antoine Delforge

Assistant en droit et chercheur au CRIDS/NADI de l'UNamur

et

Yves Poullet

Professeur émérite à l'université de Namur, professeur associé à l'UCLille et co-président du NADI

Introduction

1. Deux approches – blockchain et RGPD ; RGPD et blockchain. La contribution ambitionne deux objectifs qu'il importe de distinguer. Le premier est souvent évoqué dans la littérature : faut-il appliquer le RGPD aux infrastructures et applications blockchain et, si oui, comment faut-il interpréter certaines dispositions du RGPD confrontées à ces réalités nouvelles ? Ces questions seront développées dans un premier temps (Chapitres 1 à 4). Ensuite, nous étudierons comment il est possible de voir dans les blockchains un outil permettant de mettre en pratique certains principes du RGPD, en particulier l'obligation d'accountability et de transparence du responsable du traitement et d'amélioration de l'« *empowerment* » de la personne concernée sur l'exploitation de ses données à caractère personnel. La blockchain ne pourrait-elle pas être un de ces instruments qui permettrait de rendre plus effectif le RGPD ? C'est la question que nous aborderons dans le Chapitre 5.

2. Les questions à se poser. L'intérêt de la blockchain est fondé sur le fait que le système de registre distribué permet à chaque utilisateur

d'avoir la preuve des transactions, de préserver leur intégrité et de conserver un historique des diverses transactions[1]. On conçoit dès lors la crainte exprimée par certains vis-à-vis d'une technologie qui permet, non seulement, le traçage des transactions opérées par les utilisateurs du réseau, soit directement, soit à travers un objet dont il a la maîtrise, mais, également, vu les caractéristiques du fonctionnement des blockchains, l'impossibilité de modifier les registres des transactions et donc des données à caractère personnel y contenues, sans respect des droits à la correction et à l'effacement conférés à la personne concernée par le RGPD. Par ailleurs, la recherche du responsable des traitements engendrés par le fonctionnement des blockchains soulève une question majeure : qui peut et doit être considéré comme responsable de ces traitements ? Autre point : comment aborder le fait que les réseaux des blockchains sont internationaux et ne s'arrêtent pas aux frontières européennes ?

Nombre d'auteurs[2] s'interrogent dès lors sur la conformité des applications de la blockchain au Règlement européen général sur la protection

[1] À cet égard, voy. le Rapport du 20 juin 2018 n° 584 (2017-2018) adressé au Sénat de la République française de Mme V. Faure-Muntian, député, MM. C. De Ganay, député et R. Le Gleut, sénateur, rapport fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, sous le titre « Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies ».

[2] Voy. S. Stankovitch, « GDPR vs Blockchain – Technology Against The Law », disp. sur https://cryptobriefing.com/gdpr-vs-blockchain-technology-against-the-law/ ; C. Kuner, F. Cate, O. Linksey, C. Millard, N. Niloidean et D. Svantesson, « Blockchain versus data protection », *Int. Data Privacy Law*, 2018, vol. 8, issue n° 2, pp. 103 et s. : « *So, as many issues that arise in data protection law, the appropriate answer to the question... is not binary but rather: 'it depends'* ». À propos des doutes soulevés par nombre d'auteurs, voy. l'étude réalisée en juillet 2019 par M. Finck, *Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?*, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service. Le sommaire de l'étude rejoint notre propos : « *Blockchain is a much-discussed instrument that, according to some, promises to inaugurate a new era of data storage and code-execution, which could, in turn, stimulate new business models and markets. The precise impact of the technology is, of course, hard to anticipate with certainty, in particular as many remain sceptical of blockchain's potential impact. In recent times, there has been much discussion in policy circles, academia and the private sector regarding the tension between blockchain and the European Union's General Data Protection Regulation (GDPR). Indeed, many of the points of tension between blockchain and the GDPR are due to two overarching factors. First, the GDPR is based on an underlying assumption that in relation to each personal data point there is at least one natural or legal person – the data controller – whom data subjects can address to enforce their rights under EU data protection law. These data controllers must comply with the GDPR's obligations. Blockchains, however, are distributed databases that often seek to achieve decentralisation by replacing a unitary actor with many different players. The lack of consensus as to how (joint-) controllership ought to be defined hampers the allocation of responsibility and accountability. Second, the GDPR is based on the assumption that data can be modified or erased where necessary to comply with legal requirements, such as Articles 16 and 17 GDPR. Blockchains, however, render*

des données (en abrégé, le RGPD), récemment entré en application[3]. Sans doute aurons-nous l'occasion de souligner les difficultés soulevées par la mise en œuvre des principes issus du règlement dans le cadre de la technologie de la blockchain ; encore faut-il préalablement se poser une question préjudicielle : le règlement s'applique-t-il ? Les transactions concernées par la blockchain concernent indiscutablement des personnes, et bien souvent des individus, qu'il s'agisse de transactions d'assurance, de locations d'immeubles, de certificats de la qualité professionnelle ou autres ; pour autant, y a-t-il traitement de données à caractère personnel ?

3. Réflexions liminaires. Avant d'aborder cette question préjudicielle liée au champ d'application du RGPD, quelques réflexions. La variété des infrastructures de blockchains et des applications y développées oblige à reconnaître que la réponse aux questions que nous venons de poser peut différer grandement. Ainsi, les contributions précédentes ont distingué, sans que nous revenions sur leurs développements, les blockchains publiques et celles privées et, plus précisément, celles dites « *permissionless* » et celles qui nécessitent une autorisation d'utilisation. On sait, par ailleurs que viennent se greffer sur des blockchains par ailleurs publiques, des applications blockchains développées par des opérateurs privés et réservées à des associations professionnelles ou à des groupes d'entreprises. En ce qui concerne les applications, elles sont multiples : depuis des applications développées par l'État et liées à un service public aux citoyens jusqu'à des applications privées mono-partenaire comme l'était l'application AXA[4].

On s'interrogera également sur l'objet de la certification : on conçoit en effet que certifier l'existence d'un diplôme présente moins de risques en matière de vie privée que ceux liés au contenu de polices d'assurance-vie ou à des questions de transactions immobilières.

---

the unilateral modification of data purposefully onerous in order to ensure data integrity and to increase trust in the network. Furthermore, blockchains underline the challenges of adhering to the requirements of data minimisation and purpose limitation in the current form of the data economy. This study examines the European data protection framework and applies it to blockchain technologies so as to document these tensions. It also highlights the fact that blockchain may help further some of the GDPR's objectives. Concrete policy options are developed on the basis of this analysis ». L'étude est disponible sur https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[3] Règl. (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.*, L 119, 4 mai 2016, pp. 1-88. Il est entré en application le 25 mai 2018.

[4] https://www.axa.com/fr/magazine/axa-se-lance-sur-la-blockchain-avec-fizzy.

Enfin, les smart contracts, liés à des applications blockchain font intervenir un tiers et soulèvent la question de l'automaticité des décisions prises suite à leurs déclenchements. Les DAO (*Decentralized Autonomous Organization)*, qui définissent et automatisent les règles de gouvernance de la blockchain, les inscrivant de façon immuable et transparente[5], apparaissent comme le lieu idéal d'expression des règles de vie privée. Cette autoréglementation constitue, à notre avis, le point d'entrée à privilégier et doit traduire les exigences de la réglementation et de ses exigences, à condition, bien évidemment, que son écriture ne soit pas qu'algorithmique, mais permette à la personne concernée d'accéder via un langage compréhensible à l'intelligence du fonctionnement de la blockchain. La personne contrôlée pourra ainsi contrôler le respect de la législation (RGPD) et, en particulier de ses droits.

CHAPITRE 1. L'applicabilité du RGPD aux blockchains

4. Une question préjudicielle : blockchain et données à caractère personnel. Le RGPD s'applique aux traitements de données à caractère personnel. L'article 4 du RGPD définit largement la notion de données à caractère personnel comme toute information se rapportant à une personne physique identifiée ou identifiable, y compris par référence à un identifiant, ou à un ou plusieurs éléments spécifiques propres à son identité[6]. Pour faire bref, on peut considérer qu'est donnée à caractère personnel toute information qui, en raison de son contenu, finalité ou de son impact, peut être liée à une personne individualisée même si celle-ci n'est pas identifiée par son nom. Le RGPD exclut de son champ d'application les données anonymes[7].

[5] « C'est une forme d'organisation incorruptible qui appartient aux personnes qui ont aidé à la créer et à la financer, et dont les règles sont publiques… Il n'y a donc pas besoin de faire confiance à qui que ce soit, car tout est dans le code » détaille Stephan Tual, co-créateur du projet TheDAO. Cette définition est reprise par le site de Blockchain France : https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/.

[6] Voy. art. 4, 1), RGPD. Le Groupe de travail article 29 (prédécesseur sous la directive 95/46 de l'actuelle EDPB (European Data Protection Board)) avait, dès 2007, proposé une interprétation de la notion dans son *Opinion 04/2007 on the concept of personal data*, WP 136, 20 juin 2007.

[7] On sait que de plus en plus de scientifiques considèrent que cette distinction n'est plus de mise à l'heure où la puissance de nos ordinateurs et en particulier des systèmes d'intelligence artificielle permettent de faire « sauter » le soi-disant anonymat de nombre de données agrégées et prétendues anonymes. Sur cette question, voy. déjà en 2000,

Certaines applications de la blockchain ont pour objet, à leur demande, la certification de la qualité d'individus : leur qualité de propriétaire, d'étudiant... certains éléments de leur identité civile ou leur statut au sein d'une entreprise ou association. Ces applications sont bien évidemment soumises aux législations sur les données à caractère personnel. Il n'en reste pas moins que la plupart des applications utilisent des données soigneusement cryptées y compris dans l'adresse des émetteurs et destinataires et dans les contenus véhiculés. Certes, ces données peuvent être décryptées ou une fois mises en relation avec un contenu lisible, attestent de leur authenticité. Faut-il dès lors à leur propos parler de données à caractère personnel et leur appliquer le RGPD ? C'est la question qui retiendra notre attention.

Entre données qui permettent une identification directe et données anonymes qui exclut toute identification au sens le plus large des personnes, le RGPD introduit la notion de données pseudonymes ou, pour être plus exact, décrit le processus de pseudonymisation, car c'est bien ainsi que l'article aborde la question des données pseudonymisées. Par pseudonymisation, on entend « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[8]. En d'autres termes, le RGPD ne tranche pas la question de savoir si la donnée pseudonymisée est ou non donnée à caractère personnel, mais décrit une méthode de diminution de risque. Certains auteurs[9], et en particulier le Groupe de travail article 29, estiment que la donnée pseudonymisée reste

---

L. Sweeney, « Simple Demographics Often Identify People Uniquely' Data Privacy », *Working Paper* 3, disp. sur https://dataprivacylab.org/projects/identifiability/paper1.pdf ; A. Narayanan et V. Shmatikov, « Myths and Fallacies of "Personally Identifiable Information" », *Communications of the ACM*, juin 2010, vol. 53, n° 6, pp. 24 et s.

[8] Art. 4, 5), RGPD.

[9] P. Ohm, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », *UCLA Law Review*, 2010, vol. 57, p. 1701 ; M. Veal *et al*, « When data protection by design and data subject rights clash », *International Data Privacy Law* 2018, n° 8, en particulier, p. 113 ; N. Eichler et T. Jansen, « Blockchain and Data protection Law : When anonymous data becomes personal », disp. sur https://www.dotmagazine.online/safe-xmas/whos-naughty-now-can-santas-business-model-survive-the-gdpr/blockchain-and-data-protection-law-when-anonymous-data-becomes-personal : « *At first sight, data stored on a blockchain appear to be anonymous, consisting mostly of hashed values and cryptic wallet ID numbers which cannot be directly linked back to the individual to which they relate. As a result, some may assume that, due to the apparent anonymity, there is no room for the application of*

une donnée à caractère personnel même si son traitement peut présenter peu de risques de réversibilité du processus de pseudonymisation vu la qualité des parties qui y ont procédé (elles peuvent être tenues par un secret professionnel) et la sécurité des méthodes utilisées[10].

À l'inverse, s'appuyant sur le considérant n° 26 du RGPD[11], la plupart des auteurs[12] y compris certaines autorités de protection des données[13] estiment que la pseudonymisation peut conduire à l'anonymisation et donc à la non-application du RGPD lorsqu'il sera nécessaire de recourir à des moyens « déraisonnables » pour remonter aux personnes concernées.

5. Anonymisation et/ou pseudonymisation ? Dans la plupart des applications blockchain, les transactions reprises dans le registre mentionnent l'émetteur et le destinataire, mais sous la forme d'une signature électronique et les contenus qui pourraient également contenir des données à caractère personnel sont sévèrement cryptées et ne contiennent que le résultat illisible sauf au destinataire légitime du message que le résultat d'un « hashage » lié à l'utilisation de signatures cryptographiques soit asymétriques à clé publique, soit échangées de manière strictement confidentielle entre membres d'un consortium ayant décidé d'utiliser le

---

European data protection laws. In fact, a closer look at European data protection laws pertaining to the identifiability of an individual person reveals that data stored on a blockchain may not be considered anonymous, but as personal data, because the individual person is identifiable ».

[10] C'est la théorie du risque zéro qui est ainsi défendue, en particulier par le Groupe dit de l'article 29 dans l'opinion déjà citée, mais également dans celle de 2014 précisément sur les techniques d'anonymisation, voy. *Opinion 05/2014 on Anonymisation Techniques*, WP 216, 10 avril 2014, p. 3.

[11] « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable ».

[12] Sur ce débat et la position plus souple adoptée par de nombreux auteurs, voy. S. Stall, A. Bourdillon et A. Knight, « Anonymous data v. personal data – a false debate : an EU perspective on anonymization, pseudonymization and personal data », *Wisconsin International Law Journal*, 2018, 34 (2), pp. 284-322.

[13] Ainsi, le rapport au Parlement européen précité (note n° 3) fait notamment référence à des décisions et opinions émises par les autorités de protection des données autrichiennes et du Royaume-Uni.

système de la blockchain. La présence et l'accès à ces données « cryptées ou hashées permettent-ils d'identifier les individus qui se cachent derrière ces signatures »[14] ? Sans doute la réponse variera : s'il s'agit de la personne ayant crypté et donc ayant les moyens de décrypter ou du destinataire auquel l'émetteur du message a donné les moyens de décrypter, il est clair que les données originellement à caractère personnel restent à caractère personnel[15]. Pour les tiers *a priori* interdits d'accès aux messages et à leur contenu, l'application ou non du RGPD dépendra de la qualité de la clé utilisée et de la fréquence de sa mise à jour. Certains systèmes de signature permettent d'ailleurs de générer, à chaque opération, une signature nouvelle, ce qui rend le décryptage de la signature privée tant de l'émetteur que du destinataire difficile.

Il s'agira en définitive de constater si, oui ou non, par des moyens « raisonnables », l'identification des personnes concernées est possible[16]. À cet égard, deux théories s'affrontent : l'une, dite "objective" renvoie à la question de l'« identifiabilité » en soi des données ; l'autre, dite « subjective », prend en compte les moyens que la personne qui accède aux données, seule ou avec l'aide d'autrui, peut raisonnablement mettre en œuvre. Cette seconde conception a l'appui de la Cour de justice qui, dans l'affaire *Breyer*[17], a considéré que l'adresse IP dynamique n'était pas nécessairement une donnée à caractère personnel dans la mesure où celui qui détient cette donnée peut démontrer qu'un ou plusieurs tiers[18] n'ont pas raisonnablement les moyens de relier cette adresse IP à une personne identifiable. Si l'on suit cette lecture » subjective », il faudra dans certains cas conclure, du moins si on s'en tient aux seules données présentes dans la chaîne et accessibles à tous les utilisateurs de la chaîne, que les données

[14] Comme le notent à propos de la blockchain Bitcoin P. DE FILIPPI et M. REYMOND, voy. « La Blockchain : comment réguler sans autorité », in T. NITOT, T. et N. CERCY (dir.), *Numérique : reprendre le contrôle*, Paris, Framabook, 2016, p. 81 : « les individus qui font des échanges en Bitcoin ne sont désignés dans la blockchain qu'à travers leur adresse Bitcoin, un identifiant global sous forme d'une chaîne de caractères de ce type : 37WctrDb1G1orXhJ8vgx7zS2WCuSuBk6EQ. Aucune autre information n'est disponible, ni sur leur identité hors ligne, ni sur la nature de leur transaction ».

[15] À ce propos, voy. GROUPE DE TRAVAIL ARTICLE 29, *Opinion 05/2012 sur le Cloud Computing*, WP 196, 1er juillet 2012.

[16] Sur cette question, voy. V.L. SLAAN, « Privacy issues by blockchain: hoe voorkom of minimaliseerje die? », *Computerrecht*, 2017, p. 255.

[17] C.J.U.E., 19 octobre 2016, arrêt *Breyer*, C-582/14.

[18] « *There is no requirement that all the information enabling the identification of the data subject must be in the hands of one person* » (arrêt *Breyer*, précité, § 31). Sur ce point, voy. T. BUOCZ *et al.*, « Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks », *Computer Law & Security* Review, 2019, n° 1, p. 9.

des registres distribués sont anonymes[19] (on imagine mal le commerçant lever les secrets de la cryptographie mise en œuvre, suite au paiement en bitcoin qui lui est adressé). Notre réflexion n'exclut pas que la levée de l'anonymat ait lieu du fait de données circulant hors chaîne (ainsi, si l'utilisateur d'une blockchain utilise sa connexion et donc révèle l'adresse IP; ainsi, si le commerçant peut avoir reçu un courriel précédant la commande et le paiement en bitcoin lui permet de lever le secret; enfin, si les législations anti-blanchiment ou les exigences réglementaires liées à l'obligation bancaire peuvent exiger la transmission des clés publiques des personnes émettrices ou destinataires du message aux autorités bancaires voire publiques de contrôle)[20]. Enfin, on sait que les progrès des développements informatiques rendent désormais possible la réidentification de données « hachées »[21]. Par ailleurs, la CNIL[22], dans ses « *Premiers éléments d'analyse* », estime que les clés publiques utilisées dans le cadre des

[19] En ce sens, voy. le rapport de décembre 2015 du Conseiller scientifique du gouvernement anglais rédigé par M. Walport, Chief Scientific Advisor to HM Government, *Distributed Ledger Technology. Beyond Block Chain*, p. 50, disp. Sur https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[20] Sur ces hypothèses, lire D.-A. Sauvage, *La blockchain face au droit à l'effacement*, Travail de fin d'études, DTIC, Université de Namur, pp. 4 et s. ; Rapport du Parlement européen, précité en note n° 3, p. 39 : « *Academic research has also confirmed that public keys can be traced back to IP addresses, aiding identification. Where a user transmits a transaction to the network, they usually connect directly to the network and reveal their IP address Law enforcement agencies across the world have moreover identified individuals through their public keys through forensic chain analysis techniques to identify suspected criminals on the basis of their public keys, and a range of professional service providers performing related services have emerged* ». On note que certains législateurs précisément pour éviter que les cryptomonnaies puissent servir d'instruments de blanchiment d'argent interdisent ou envisagent d'interdire l'utilisation de systèmes de cryptage, tel que le *zero-knowledge*. Voy. le cas français : Assemblée Nationale, *Rapport d'Information par la Commission des Finances, de l'Économie Générale et du Contrôle Budgétaire relative aux monnaies virtuelles*, 30 janvier 2019, en particulier p. 246, disp. sur http://www.assemblee-nationale.fr/15/pdf/rap-info/i1624.pdf ; à propos de la même volonté au Japon, voy. W. Suberg, « Japanese Regulatory Discussed Restricting Trade of Privacy-Focused Altcoins, Report Says », disp. sur https://cointelegraph.com/news/japanese-regulators-discussed-restricting-trade-of-privacy-focused-altcoins-reportsays.

[21] Sur ce point, voy. le rapport au Parlement européen cité précédemment (note n° 3) ; G. Acar, « Four cents to deanonymize: Companies reverse hashed email addresses », disp. sur https://freedom-totinker.com/2018/04/09/four-cents-to-deanonymize-companies.reverse-hashed-email-addresses/202 ; E. Felten, « Does Hashing Make Data "Anonymous" », disp. sur https://www.ftc.gov/newsevents/blogs/techftc/2012/04/does-hashing-make-data-anonymous.

[22] Commission Nationale de l'Informatique et des Libertés, *Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données à caractère personnel*, septembre 2018, disp. sur https://www.cnil.fr/fr/blockchain-and-gdpr-solutionsresponsible-use-blockchain-context-personal-data.

blockchains sont des données à caractère personnel dans la mesure où « l'architecture même de la blockchain fait que ces identifiants seront toujours visibles, car ils sont indispensables à son fonctionnement ». En cas de contestation sur le caractère anonymisé des données grâce aux techniques de signature et de hashage utilisées, il appartiendra aux responsables du traitement, à démontrer ce caractère anonyme, ce qui au regard de l'évolution rapide des techniques de décryptage et des applications de l'intelligence artificielle risque d'être de plus en plus problématique. Le renvoi à ce devoir de preuve oblige à s'interroger sur la personne « *accountable* » : qui est responsable du ou des traitements générés par le fonctionnement de la blockchain ? Et de manière plus large comment qualifier au regard des concepts utilisés par le RGPD, à savoir ceux de responsable des traitements et de sous-traitants chacun ou certains des nombreux acteurs de la blockchain ?

6. L'exception à des fins strictement personnelles ou domestiques. Dans certains cas, le responsable du traitement peut bénéficier de l'exception pour traitement de données à des fins strictement personnelles ou domestiques et ainsi échapper aux obligations imposées par le RGPD et au respect des droits accordés aux personnes concernées[23]. Cette exception s'appliquera lorsque le responsable du traitement traite ces données à caractère personnel dans un but strictement personnel (non commercial ou professionnel) et qu'il ne rend pas accessible ces données à un nombre indéterminé de personnes[24]. Certaines blockchains pourraient éventuellement ne pas être soumises au RGPD. Cette hypothèse reste cependant exceptionnelle. Ainsi, si nous prenons comme exemple l'utilisation par un individu, à des fins purement privées, de la blockchain Bitcoin[25], il est loin d'être évident que l'exception prévue par le RGPD s'applique. S'il est vrai, en effet, que ce traitement n'est pas effectué à des fins professionnelles, certaines informations (les informations transactionnelles) sont rendues publiques à toute personne pouvant accéder à cette blockchain[26]

[23] Art. 2, § 2, c), et consid. 18, RGPD.

[24] Cette seconde condition a été rajoutée par la Cour de justice, voy. 6 novembre 2003, arrêt *Lindqvist*, C-101/01, pt 47 ; 11 décembre 2014 arrêt *František Ryneš c. Úřad pro ochranu osobních údajů*, C-212/13 ; 14 février 2019, arrêt *Augstākā tiesa*, C-345/17). À ce sujet voy. C. DE TERWANGNE, « Définitions clés et champ d'application du RGPD », in C. DE TERWANGE et K. ROSIER (dir.), *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie*, coll. du CRIDS, n° 44, Bruxelles, Larcier, 2018, p. 71.

[25] Exemple repris à la Commission Nationale Informatique et Libertés dans « Premiers Éléments d'analyse de la CNIL : Blockchain », disp. sur https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

[26] Ce nombre de personnes et le type de personnes pouvant y accéder variera en fonction du type de blockchain.

et donc la seconde condition pour pouvoir bénéficier de cette exception pourrait faire défaut[27]. À cela s'ajoute naturellement la question de savoir si ces données transactionnelles sont bien des données à caractère personnel[28].

Notons que, quand bien même cette exception s'appliquerait, le RGPD continuerait tout de même à s'appliquer puisque le considérant 18 précise bien que « le règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques »[29]. Les personnes qui mettent à disposition cette blockchain et en assurent le bon fonctionnement pourraient ainsi encore être soumises au RGPD et notamment aux obligations en matière de sécurité. De fait, si le responsable du traitement « exonéré » n'est plus soumis au respect des règles du RGPD, il n'en reste pas moins vrai que son sous-traitant ou son responsable conjoint « non exonéré »[30] devra toujours respecter l'ensemble du RGPD, sans exception. Cette assertion n'est d'ailleurs pas sans poser certaines difficultés (signature de contrats[31], coopération, échange d'information...) dans la mesure où il semble peu évident pour un sous-traitant ou un responsable conjoint de pouvoir respecter ses propres obligations quand leur est imposée l'obligation de coopérer avec un responsable du traitement qui n'est pas tenu de respecter le RGPD. Sur ce point, une solution spécifique à la blockchain devrait être trouvée par une interprétation du texte du RGPD.

7. L'applicabilité territoriale du RGPD. Sans rentrer trop dans les détails[32], le RGPD s'appliquera dans deux hypothèses : lorsque le sous-traitant ou le responsable du traitement est établi au sein de l'UE ou lorsque celui-ci cible des personnes concernées établies au sein de l'UE[33].

---

[27] Dans ce sens, Rapport du Parlement européen, précité en note n° 3, p. 13.

[28] Voy. *supra*, § 4.

[29] Nous employons ici le conditionnel dans la mesure où la portée réelle de ce considérant reste actuellement discutée. Voy. A. DELFORGE, « Les obligations générales du responsable du traitement et la place du sous-traitant », in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie*, *op. cit.*, p. 395.

[30] Voy. *infra*, Chapitre 2 pour comprendre quels types d'acteurs peuvent tomber dans ces catégories.

[31] Art. 26 et 28 RGPD, voy. *infra*, § 14.

[32] Pour plus de précision, voy. EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR*, 7 janvier 2018.

[33] Art. 3, § 2, RGPD : « Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces

Pour les blockchains publiques, le RGPD s'appliquera donc *a priori* dans la mesure où de par leur nature internationale, il y a de fortes chances que certains traitements soient effectués par certaines personnes établies en Europe, et que ces blockchains visent un public mondial et donc des citoyens européens. Nous pensons notamment à blockchain Bitcoin qui n'a pas véritablement de restriction géographique.

La seule manière d'y échapper serait d'imposer certaines restrictions visant à interdire l'utilisation de la blockchain aux personnes établies en Europe et interdire de traiter des données venant de citoyens européens. Cela semble assez peu réaliste. Pour les blockchains privées ou semi-privées, elles sont généralement plus circonscrites à un territoire spécifique et il est donc plus facile de déterminer si le RGPD s'applique ou non. Par exemple, pour une blockchain (privée ou semi-privée) utilisée à des fins de traçabilité des produits dans une chaîne de distribution alimentaire, il est relativement facile de déterminer si des données à caractère personnel de citoyens européens vont être traitées (ainsi, les noms des fournisseurs...) sur base de l'implantation géographique des personnes impliquées dans cette chaîne de production.

Une autre manière de raisonner, probablement plus pertinente pour éviter une applicabilité parfois illogique du RGPD à des cas sans rapport avec l'UE, serait d'envisager une segmentation par transaction. La blockchain n'est donc pas dans sa globalité soumise ou non au RGPD, mais seules certaines transactions ayant un élément de rattachement avec l'UE seraient soumises aux prescrits de ce règlement. Par exemple, une blockchain publique pensée pour être utilisée par des Américains ne serait pas « contaminée par le RGPD » dans son entièreté du seul fait que quelques sociétés européennes l'utilisent également pour assurer la traçabilité de certaines transactions. Dans ce cas, seules les transactions effectuées par des entités établies dans l'Union européenne, ou ciblant un public européen (par exemple au regard de la publicité opérée par l'opérateur de la blockchain), seront soumises au RGPD, et non la blockchain dans son ensemble. L'important est donc de vérifier quel est le « public cible » de chaque blockchain[34].

---

personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

[34] Cette logique qui vise à ne pas appliquer ou à n'appliquer que partiellement le RGPD est la même que celle tenue au sujet de fournisseur de service Cloud au niveau mondial où la question de l'applicabilité du RGPD se posait. À ce sujet, voy. M. S. VIDOVIC, « EU data protection reform : challenges for cloud computing », disp. sur http:// www.cyelp.com/index.php/cyelp/article/view/252, p. 181 ; K. HON, « GDPR : Killing Cloud Quickly ? », disp. sur https://iapp.org/news/a/gdpr-killing-cloud-quickly/.

8. La question des flux transfrontières. Précisons que si certaines données à caractère personnel sont traitées hors de l'UE, et cela s'avéra très fréquent dans le cas des blockchains, le(s) responsable(s) du traitement est(sont) alors tenu de respecter les règles en matière de flux transfrontières[35] qui visent à assurer un niveau de protection substantiellement équivalent[36] dans les pays extra-européens. Si les données circulent dans des pays considérés comme « assurant un niveau de protection adéquat »[37], cela ne pose aucun souci et le transfert peut être effectué sans autre formalité. Si ce n'est pas le cas, alors le responsable du traitement est tenu de mettre en place des « garanties appropriées »[38]. L'article 46 liste différentes formes de garanties. La plupart consistent à exiger des différents acteurs impliqués dans le transfert de s'engager contractuellement à respecter certaines règles qui reprennent les éléments essentiels du RGPD. Dans le cas des blockchains, ces règles devraient être mises en place au niveau de la DAO et s'appliquer à toutes entités souhaitant interagir avec la blockchain. On ajoute au vu de l'arrêt *Schrems II*[39] de la CJUE,

---

[35] Voy. chapitre V RGPD.

[36] Selon l'expression de la Cour de justice de l'Union européenne dans l'affaire *Schrems I* (arrêt du 6 octobre 2015, C-362/14).

[37] Ces pays ont alors fait l'objet d'une décision d'adéquation de la Commission européenne.

[38] Art. 46 RGPD. L'arrêt *Schrems II* (CJUE, 16 juillet 2020, arrêt *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, C-311/18) qui vient d'être prononcé (exige que ces garanties appropriées apportent également un niveau de protection substantiellement équivalent à celui du RGPD : « L'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du règlement 2016/679 doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne par ce règlement, lu à la lumière de la charte des droits fondamentaux de l'Union européenne. À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union européenne et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, paragraphe 2, dudit règlement ».

[39] CJUE, 16 juillet 2020, arrêt *Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems*, C-311/18. Dans cet arrêt, la Cour annule le « Pivacy Shield », c'est-à-dire un mécanisme négocié entre l'UE et les États-Unis permettant aux entreprises américaines d'effectuer, à certaines conditions, des flux de données à destination des États-Unis. Dans ce contexte, les clauses contractuelles et les BCR, mécanismes alternatifs à la reconnaissance de l'adéquation d'un pays (mécanismes prévus par les art. 46 et s. RGPD) ne suffisent plus à eux seuls pour valider un transfert vers un pays qui ne satisfait pas aux conditions d'une protection « substantiellement équivalente » à celle offerte dans l'UE.

tout récent, que les mécanismes déjà mis en place entre acteurs, et ce afin d'effectuer les flux transfrontières nécessités par la blockchain, risquent d'être remis en cause. En effet, la Cour insiste dorénavant davantage sur le caractère effectif de la protection accordée.

CHAPITRE 2. La qualification des acteurs dans une blockchain

9. Aperçu des acteurs dans une blockchain. Le fonctionnement de la blockchain nécessite nombre d'acteurs, et ce, en fonction du type même de montage requis. Les contributions précédentes ont mis en lumière la diversité de ces acteurs : ainsi, les personnes, émetteurs de messages transmettent ces derniers en direct, mais souvent via des intermédiaires en charge de les crypter voire d'en « hasher » le contenu. Les messages entrent dans des blocs. Chaque bloc est validé par certains utilisateurs baptisés « mineurs » (en référence aux chercheurs d'or), et transmis alors aux « nœuds » du réseau, c'est-à-dire aux détenteurs du registre, ce registre étant la chaîne de blocs elle-même. Cette dernière est actualisée en permanence. Dans les blockchains dites ouvertes (*permissionless*), comme celle du bitcoin, n'importe quel utilisateur de l'Internet peut ainsi devenir un nœud du réseau en téléchargeant le registre auprès d'un nœud existant. Chaque nœud est connecté à plusieurs autres, appelés pairs, eux-mêmes ayant leurs propres pairs, ce qui forme un réseau pair-à-pair. À ce schéma simple, on ajoutera bien d'autres acteurs lorsqu'il s'agit de blockchains privées ou semi-publiques. Ainsi, il est utile de noter que tantôt un consortium d'entreprises avec ou sans personnalité juridique, regroupées au sein ou non d'une association professionnelle et regroupant des entreprises concurrentes ou non, tantôt une entreprise ayant de nombreux filiales et employés, développe, avec souvent l'appui d'un concepteur, firme de consultance spécialisée dans le montage de blockchains, le système qui correspond à leurs besoins[40]. Comme le note le rapport au Sénat français[41], « il existe aussi un grand nombre de protocoles à restriction d'accès, pour certains particulièrement aboutis et déjà opérationnels. Parmi

[40] Voy. sur l'intérêt des entreprises même concurrentes à recourir à la blockchain pour des raisons de réduction des coûts transactionnels l'intéressant article de T. SCHREPEL, « The Theory Of Granularity– A Path for Antitrust in Blockchain Ecosystems », disp. sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3519032, pp. 17 et s.

[41] Rapport précité.

ces derniers, les blockchains "de consortium" résultent du regroupement de plusieurs organisations indépendantes, voire concurrentes, utilisant la blockchain pour archiver dans un registre décentralisé des transactions sécurisées, ou échanger des actes certifiés, sans avoir à faire intervenir un tiers de confiance. D'autres protocoles sont utilisés au sein d'une même organisation ou entreprise, pour simplifier et automatiser des échanges et des certifications »[42]. Quelques exemples de ces divers cas : la fédération des notaires de France a fait développer en concertation avec l'association des banques une blockchain qui garde les traces « hashées » de différents messages envoyés par les premiers aux seconds relatifs à des injonctions de paiement. Les acteurs d'une chaîne allant de la production à la distribution finale ont confié à IBM la réalisation (y compris la rédaction de la DAO) d'une chaîne de blocs fonctionnant sur une infrastructure publique de blockchain (Ethereum), permettant aux acteurs intéressés de suivre les transactions effectuées entre eux et d'en garantir la preuve par un système de registre décentralisé opéré par différents nœuds.

Ainsi, on distingue nombre d'acteurs, et ce en fonction des types de blockchains, mais également du rôle des acteurs. On pointe des acteurs situés en aval de la création de la blockchain, comme le concepteur de celle-ci. Parmi ceux qui participent directement au fonctionnement de la blockchain, on distinguera les utilisateurs actifs, c'est-à-dire les « participants » qui décident introduire des données (au sens le plus large) dans la chaîne et les soumettent à la validation des mineurs, les nœuds où sont repris les registres de blocs validés par les mineurs qui peuvent être soit identifiés, soit non identifiés au départ ; les destinataires des messages et toute autre personne qui souhaite accéder aux données conservées dans le bloc, soit parce qu'autorisée, soit en dehors de toute autorisation, dans le cas des blockchains *permissionless*. Enfin, on note les « gouvernants » de la blockchain qui, dans le cas de blockchains privées, prennent les décisions quant à l'évolution du système. Comment qualifier ces acteurs au regard des concepts utilisés par le RGPD, et d'abord celui central de « responsable du traitement » ?

10. L'identification du responsable du traitement. L'article 4.7) du RGPD envisage le responsable comme celui qui définit les finalités et les

[42] Rapport préc. : « Deux projets majeurs de *blockchains* privées méritent d'être évoqués. Le premier, Hyperledger, a été lancé il y a deux ans par la fondation Linux, et réunit aujourd'hui plus de 85 membres, dont Accenture, Airbus, Fujitsu, JP Morgan, Intel ou encore IBM. Le second est le consortium interbancaire R 3, qui se veut un registre distribué pour les services financiers. Il compte en son sein, entre autres, les établissements suivants : Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J. P. Morgan, Royal Bank of Scotland, State Street, UBS… ».

moyens du traitement, le critère de la finalité devant être pris en considération de préférence à celui de la technique[43]. Ce personnage est central. Il est « accountable » des traitements dont il est désigné responsable et veille au respect des principes définis par le règlement[44]; il informe et garantit le respect des droits des personnes concernées, en ce qui concerne l'accès, la rectification voire l'opposition aux traitements ou à des données traitées[45]. C'est lui qui prend les moyens de garantir la sécurité des traitements[46], etc. On ajoute que, selon le Groupe de travail article 29 (opinion reprise par son successeur l'EDPB), c'est la réalité qui compte et non les qualifications juridiques qu'à travers des contrats ou des DAO, on pourrait donner ou refuser de donner à certains acteurs[47].

11. Responsabilité individuelle ou conjointe. À cet égard, il nous paraît que dans nombre de blockchains privées mises en place par une ou des entreprises pour servir ses ou leurs clients, un ou des fournisseurs d'énergie, une ou des compagnies d'assurances ou, bien sûr, l'État, c'est cet acteur qui est responsable. En effet, c'est cette entreprise, ce consortium ou cette administration étatique qui décide de poursuivre via la blockchain la réalisation de finalités qui souvent préexistaient à l'établissement de la blockchain. Cette responsabilité peut être celle d'une entité, mais elle peut également être partagée. C'est alors une responsabilité conjointe, selon la définition de l'article 26 du RGPD : « lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux ». Cette qualification, récemment mise en valeur par la CJUE, en particulier dans l'affaire *Wirtschaft Akademia*[48], va de soi lorsque les blockchains sont mises en place par des communautés

[43] GROUPE DE TRAVAIL ARTICLE 29, *Opinion 1/2010 sur les concepts de responsable de traitements et de sous-traitants*, WP 169, 16 février 2010, p. 14 et tout récemment le projet de « Guidelines 07/2020 on the concepts of controller and processor in the GDPR », soumis à consultation publique le 2 septembre 2020 (projet accessible sur le site de l'EDPB).

[44] Art. 5, § 2, et 24 RGPD.

[45] Chapitre III RGPD.

[46] Art. 5, § 1, f), et art. 32 et s. RGPD.

[47] GROUPE DE TRAVAIL ARTICLE 29, *Opinion 1/2010 sur les concepts de responsable de traitements et de sous-traitants*, préc.

[48] CJUE, 5 juin 2018, arrêt *Wirtschafsakademie Schleswig-Holstein*, C-210/16, § 16. Voy. égal. l'affaire CJUE, 10 juillet 2018, arrêt *Jehovan Todistajat*, C-25/17.

d'utilisateurs[49], mais elle nous apparaît particulièrement relevante, lorsque des consortiums, même sans personnalité juridique, reprenant des acteurs parfois concurrents ou situés à des stades différents de la chaîne économique décident d'utiliser pour des raisons de diminution des coûts transactionnels une même blockchain tout en garantissant via des mécanismes de sécurité adéquats la confidentialité des messages échangés de façon à préserver la concurrence entre eux. Sur ce point nous suivons les remarques de T. Schrepel[50] (« Collusion by blockchain and smart contracts », 33, *Harvard Law Journal*, 1, 2019, pp. 118 et s.) qui à l'approche classique de la notion de consortium fondée sur l'existence soit d'une personnalité juridique, soit de contrats de coopération ou d'entente préfère parler de « collusion » de comportements indiquant une convergence de comportements, suffisante pour qu'on puisse parler de responsables conjoints. Sa théorie appliquée au droit de la concurrence doit, nous semble-t-il, trouver application également en droit de la protection des données.

12. La question de l'identification du responsable dans les blockchains publiques mises à disposition de tous. Dans ces réseaux où se multiplient les nœuds et où chacun peut accéder au registre et l'abriter, il est difficile d'identifier qui définit la finalité et les moyens comme c'est le cas lorsqu'un tiers de confiance coordonnait l'ensemble du réseau. Chaque utilisateur susceptible de décharger le registre distribué devrait alors être considéré comme responsable du traitement ou des traitements

[49] Voy. l'exemple de la communauté de personnes privées gérant en commun, grâce à une blockchain, leur production et leur consommation d'énergie ou mutualisant leurs risques sous forme d'une sorte d'assurance purement privée. Cette qualification de responsables conjoints nous paraît préférable et plus conforme à la réalité que celle proposée par le document de la CNIL « Premiers éléments d'analyse de la blockchain » déjà cité : « Lorsqu'un groupe de participants décide de mettre en œuvre un traitement ayant une finalité commune, la CNIL recommande que le responsable de traitement soit identifié en amont. Par exemple, les participants peuvent créer une personne morale sous la forme d'une association ou d'un GIE. Elles peuvent également choisir d'identifier un participant qui prend les décisions pour le groupe et de le désigner comme responsable de traitement ».

[50] T. SCHREPEL, « The Theory Of Granularity – A Path for Antitrust in Blockchain Ecosystems », *op. cit.*, : « Against this background, the present article introduces the "theory of granularity," which permits analysis of the roles played by each (group of) participant in the horizontal governance of public permissionless blockchains. On this basis, one may identify a "blockchain nucleus," i.e., a set of participants collaborating to ensure and maximize the blockchain survival by "controlling" it all together. Antitrust and competition law becomes applicable again as the nucleus serves as the basis for the definition of the relevant market and market power, the assessment of practices' legality, and liability assignment ».

qu'il initie. C'est la proposition établie par la CNIL[51] qui considère que « le participant pourra dans un certain nombre de cas être qualifié de responsable de traitement lorsqu'il est une personne physique et que le traitement est en lien avec une activité professionnelle ou commerciale [[52]] ou lorsqu'il est une personne morale qui inscrit une donnée à caractère personnel ». Il nous apparaît difficile de parler à leurs propos, comme certains auteurs le proposent, de responsable conjoint[53] dans la mesure où chacun de ces utilisateurs n'exerce pas d'influence sur les traitements d'autrui (critère mis en évidence par la CJUE dans l'affaire des témoins de Jéhovah[54]).

Une autre possibilité, en particulier dans le cas des blockchains publiques, où le nombre de personnes ayant accès aux registres distribués rend illusoire de conférer à chacun la qualité de responsable, serait, comme le laisse entendre le même document de la CNIL, de considérer que personne n'est responsable, et que, dès lors, pour que le règlement ne soit pas privé d'une partie de son effectivité, faute de personnes pouvant être tenues du non-respect des principes et dispositions de ce règlement[55], ce soit l'autorité de protection des données (laquelle ?) qui prenne les dispositions nécessaires à assurer cette effectivité. Sans doute, sur ce point, une solution réglementaire européenne serait la bienvenue. On pourrait considérer le critère subsidiaire[56] du choix des techniques utilisés par la blockchain, mais celui-ci renvoie aux choix faits par une pluralité

[51] CNIL, « Premiers éléments d'analyse de la blockchain », *op. cit.*, p. 4 : « La CNIL constate toutefois que les participants, qui ont un droit d'écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs peuvent être considérés comme responsables de traitement. ». Le mot participant doit-il s'appliquer également aux utilisateurs ayant un simple accès en lecture aux données de la blockchain (simples visiteurs) ?

[52] Il s'agit d'exclure par exemple un achat de Bitcoin pratiqué par une personne individuelle pour son propre compte. Précision ajoutée par nos soins.

[53] À cet égard et dans ce sens, V.L. Slaan, « Privacy en blockchain : wanneer is er voor wie privacy werk aan de winkel ? », *Tijdschrift voor Internetrecht*, 2017, pp. 7 et s. L'auteur y discute longuement l'avis 1/2010 sur les concepts « responsables du traitement » et « sous-traitant » émis par le Groupe de travail article 29 le 16 février 2010. Il n'en reste pas moins vrai qu'on peut difficilement imaginer qu'en tant que simple participant ayant initié deux ou trois opérations, je puisse être tenu de l'ensemble des opérations qui transitent via la blockchain.

[54] CJUE, 10 juillet 2018, arrêt *Jehovan todistajat*, C-25/17.

[55] L'hypothèse est envisagée par V.L. Slaan (cité précédemment note n° 54), même si ce dernier conclut peut-être trop vite que le règlement n'est pas applicable. À notre avis, il le reste dans la mesure où les autorités de contrôle peuvent veiller au respect des principes et dispositions et intervenir au cas où une blockchain sans responsable violerait le règlement.

[56] Dans la mesure où à la suite des opinions du Groupe de travail article 29 sur la notion de responsable du traitement, le critère du choix de la finalité devait l'emporter.

d'acteurs, les mineurs en ce qui concerne l'infrastructure de minage ou, de manière plus générale, de validation des blocs, les personnes mettant à disposition leurs serveurs comme nœuds et les divers fournisseurs de systèmes de cryptographie. Ce critère ne peut donc être d'utilité.

13. Mineurs, concepteurs, nœuds, quelle qualification pour ces acteurs ? Revenons précisément aux acteurs assumant les tâches techniques. Parmi eux, le concepteur de la blockchain qui, en fonction des préoccupations du ou des commanditaires, dessinera le système approprié à répondre aux besoins exprimés, notamment si le besoin s'en fait sentir, en incluant un mécanisme de smart contract. À leur propos, la CNIL[57] écrit : « S'agissant des smart contracts, comme pour tout logiciel, le concepteur de l'algorithme pourra être un simple fournisseur de solution ou, lorsqu'il participe au traitement, être qualifié de sous-traitant ou de responsable de traitement en fonction de son rôle dans la détermination des finalités ». Cette prise de position exige de clarifier la distinction entre sous-traitant et responsable de traitement. Le Groupe de travail article 29 insiste sur trois critères : la marge de manœuvre laissée ou non au sous-traitant, le contrôle de l'exécution du sous-traitant, la visibilité de chacun vis-à-vis des tiers. L'analyse de l'application de ces trois critères pourrait laisser apparaître qu'un concepteur qui serait le vrai initiateur d'un projet de blockchain utilisé par le consortium, dont le rôle dans la gouvernance serait important et dont la visibilité de l'apport à l'extérieur serait importante, est en réalité un responsable conjoint. On sait que le RGPD a multiplié les devoirs et obligations du sous-traitant, mais il n'en reste pas moins vrai que la responsabilité finale repose sur le responsable de traitement[58].

De ce premier cas, on distinguera l'hypothèse d'une société mettant un service de blockchain à disposition de clients. Indubitablement, cette société doit être qualifiée au moins de sous-traitant : « *By implication, it seems likely that companies offering blockchain as a service ("BaaS") also likely qualify as data processors* »[59]. La question de la qualification des nœuds

[57] GROUPE DE TRAVAIL ARTICLE 29, *Opinion 1/2010 sur les concepts de responsable de traitements et de sous-traitants*, préc., pp. 4 et 5 ; de manière beaucoup plus nuancée, le Rapport au Parlement européen déjà cité (note n° 3), pp. 67 et s.

[58] À tel point que le principe de « privacy by design » ne doit pas formellement être respecté par le concepteur de l'infrastructure si celui-ci n'est pas également considéré, au sens du RGPD, comme le responsable du traitement ou le sous-traitant, art. 25 du RGPD. Pour plus de détails sur l'obligation de « *privacy by design* », voy. A. DELFORGE, « Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, pp. 386 et s. et références citées.

[59] Rapport au Parlement européen, précité (note n° 3), p. 70.

semble devoir être résolue simplement, mais également pragmatiquement (vu leur caractère non stable et indéterminé et l'absence de marge de manœuvre qui leur est laissée) par la qualification de « tiers », que l'article 4.10 du RGPD définit comme suit : « une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe[60] du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ». Quant aux « mineurs », on retient que leur marge de manœuvre dans la validation des blocs et leur rôle dans le fonctionnement de la blockchain pourrait nous amener à préférer la qualification de sous-traitants et ce faisant, comme le suggère la CNIL dans ses « Premiers éléments d'analyse », l'éventuelle exigence de contractualisation avec les responsables de traitements ou directement les APD[61].

14. La contractualisation des relations. Par ailleurs, l'article 26 et 28.3 du RGPD exige dorénavant qu'un contrat lie les responsables conjoints entre eux, et les responsables du traitement au(x) sous-traitant(s), et ce avec un contenu précis et fort détaillé[62]. On ne cache pas les difficultés pratiques que cela poserait, en particulier lorsqu'il s'agit de mineurs utilisant le système de la « *proof of work* » où le « minage » s'opère par des consortiums changeants et souvent situés en terre lointaine[63].

Techniquement, cela reste envisageable à implémenter. Cette contractualisation se ferait de manière automatique et préalable à toute opération technique sur la blockchain, au moment de l'« inscription sur la plateforme ». Toutefois, en plus du fait qu'il semble peu probable que ce contrat soit bien rédigé et suffisamment détaillé vu la liste précise des éléments qu'il doit contenir, le caractère bien souvent relativement

[60] Ce critère « placé sous l'autorité directe » est peut-être plus discutable, mais il est certain que la marge de manœuvre des nœuds y compris lorsque ces nœuds sont identifiés *a priori* (cas de certaines blockchains privées) est particulièrement faible au vu des techniques et du rôle à jouer.

[61] CNIL, « Premiers éléments d'analyse de la CNIL : Blockchain » : « Dans le cas de la Blockchain publique, la CNIL mène actuellement une réflexion et encourage le développement de solutions permettant un encadrement des relations contractuelles entre participants/responsables de traitement et mineurs ».

[62] Voy. la liste reprise à l'article 28 du RGPD pour le contrat avec les sous-traitants. Dans celle-ci, figure notamment une série d'information sur le traitement de données effectué, l'obligation pour le sous-traitant de ne traiter les données que conformément aux ordres du responsable du traitement, l'obligation pour le sous-traitant de respecter ses propres obligations, notamment en matière de sécurité, et de garantir la confidentialité des données transmises...

[63] Le « minage » est devenu une spécialité chinoise !

anonyme des acteurs dans une blockchain (en particulier pour les blockchains publiques) rend toute contractualisation des relations impensable, voire contreproductive. Savoir avec qui on doit passer contrat s'avère impossible et il est dès lors exclu de pouvoir faire peser une quelconque responsabilité sur ces personnes anonymes (comment agir contre ce type de personne ?). C'est d'ailleurs le principe même de la blockchain, ne pas avoir besoin de faire confiance à des individus inconnus, mais uniquement dans les vertus du système technologique mis en place. Dès lors, la logique du RGPD qui impose au responsable de traitement de choisir un sous-traitant fiable, de qualité, responsable... et que l'on contractualise les obligations réciproques dans un contrat est difficilement compatible avec la logique de la blockchain. Ici, ce n'est plus « *Contract is law* », mais « *Code is Law* », pour reprendre une expression bien connue. Le respect des règles ne vient plus uniquement d'une obligation légale et/ou contractuelle, mais d'une relative impossibilité technique de s'en écarter. Il s'avérera donc probablement difficile de respecter à la lettre les prescrits de l'article 28 du RGPD, mais, au final, une blockchain, de par son *design*, assure que le sous-traitant ne peut faire autrement que respecter les règles reprises à l'article 28, ou leur esprit tout du moins. Ceci peut être vu comme une forme de mesure « *privacy by design* » dans les relations avec les sous-traitants. Certes, cela suppose – et nous y reviendrons – qu'il soit procédé à une évaluation précise des risques liés au fonctionnement de la blockchain et que les solutions technologiques prises par ceux qui mettent en place l'infrastructure soient adéquates et fassent l'objet d'une évaluation tant *a priori* qu'*a posteriori* dans les conditions de l'article 35 du RGPD qui prescrit la réalisation d'un *Privacy Impact Assessment* lorsque le niveau de risque pour la personne concernée est élevé. C'est à cette condition que l'on pourrait éventuellement renoncer à la contractualisation.

CHAPITRE 3. Les bases de licéité

15. Les bases de licéité possibles. Tout traitement de données doit reposer sur l'une des bases de licéité prévue à l'article 6 du RGPD[64], ou

[64] Le consentement de la personne, la nécessité pour l'exécution d'un contrat avec cette personne, une obligation légale, l'intérêt légitime du responsable du traitement, la nécessité au regard d'une mission d'intérêt public... Pour une liste exhaustive et mot à mot, nous renvoyons à l'article 6 du RGPD.

l'article 9 pour les données dites « sensibles »[65] [66]. Vu la diversité des blockchains et des nombreuses manières dont celles-ci sont intégrées dans l'infrastructure existante du responsable du traitement, il ne nous paraît pas opportun d'étudier en détail ces différentes bases de licéité. Toutefois, il nous semble utile d'expliquer le cheminement à adopter avant d'intégrer une blockchain dans son infrastructure.

S'il veut mettre en place une blockchain où seront traitées des données à caractère personnel, le responsable du traitement doit fonder son traitement sur l'une des bases de licéité. Dans certains cas, cette blockchain vise à proposer un nouveau service (une nouvelle finalité) à ces clients (aux personnes concernées) où la blockchain est un des éléments majeurs de ce nouveau service (ex. : vente/achat de cryptomonnaie, assurance impliquant un smart contract...). Dans ces cas, le traitement de données reposera probablement sur la nécessité de l'exécution du contrat qui unit le responsable du traitement et son client (la personne concernée), ou éventuellement le consentement de la personne concernée[67]. À l'inverse, si cette nouvelle blockchain ne s'inscrit pas dans la création d'un nouveau service au client, mais plutôt la mise en place de nouvelles technologies en « back office », doit-il forcément repasser par la personne concernée pour obtenir son approbation (sous forme d'un contrat, ou un consentement) ? Premièrement, il doit vérifier si la blockchain s'inscrit dans une nouvelle finalité (quelque chose que la société ne faisait pas avant). Si ce n'est pas le cas (la blockchain remplace autre chose qui existait déjà), il doit s'assurer, en fonction de la base de licéité utilisée que les informations communiquées à la personne concernée sont toujours pertinentes, et que le traitement est bien « nécessaire » (pas simplement plus utile pour le responsable du traitement[68]) pour l'exécution du contrat. Si ce n'est pas le cas, il peut fonder son traitement sur ses intérêts légitimes, « à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la

[65] Les données portant sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, les données génétiques, les données biométriques, les données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle...

[66] Nous n'étudierons pas, dans le cadre de cette contribution, les bases de licéité spécifiques à cet article.

[67] À éviter si possible pour le responsable dans la mesure où cela s'avère plus contraignant pour lui (davantage d'information à communiquer...), sans parler de la problématique des consentements « conditionnels » (« si tu ne consens pas, tu n'as pas accès au service »), voy. EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, v.1.1, 4 mai 2020.

[68] Il ne faut pas que des traitements de données plus importants soient nécessaires, par rapport à ce qui existait avant. Si c'est le cas, il faut trouver une autre base de licéité.

personne concernée qui exigent une protection des données à caractère personnel [...] »[69].

CHAPITRE 4. Les droits des personnes concernées

16. Préambule. Si la qualification des acteurs n'est pas chose aisée, si la mise en place pratique de certaines obligations de compliance est compliquée vu la volatilité des acteurs impliqués dans une blockchain, différentes questions restent ouvertes concernant les droits des personnes concernées. Comment gérer le droit à la portabilité exigée par le règlement en son article 20, droit qui devrait permettre à chaque utilisateur de reprendre ses données et de passer d'une blockchain à une autre ? La question n'est pas prête d'être résolue, alors même que l'interopérabilité des blockchains reste à construire. Le droit à l'oubli qui permet d'exiger l'effacement des données pose également question alors même que l'économie de la technologie de la blockchain repose sur l'immutabilité des écritures conservées dans le registre : « comme a pu l'indiquer l'Open Data Institute (ODI) britannique, pour supprimer une donnée, il faudrait que plus de la moitié des nœuds du réseau travaillent ensemble pour reconstruire la chaîne de blocs depuis le moment où la donnée a été ajoutée. Et pendant ce temps de résilience, qui peut être relativement long selon la taille de la blockchain, la donnée n'est pas actualisée. Surtout, cela signifie que toutes les données postérieurement enregistrées sur la blockchain seraient supprimées. Le risque, pour l'ODI, est alors que les données fausses ou incomplètes restent simplement sur la blockchain afin d'éviter que les données postérieures soient endommagées et perturbent le fonctionnement des programmes »[70].

17. Blockchain vs droits à la rectification et à l'effacement. Un dernier point est souvent soulevé lorsqu'est admise l'applicabilité du RGPD : celui du droit à la rectification, droit traditionnel reconnu par l'article 16 du RGPD et celui plus nouveau, du droit à l'effacement[71],

[69] Art. 6.1.f) RGPD.

[70] Voy. http://www.droit-blockchain.fr/blockchain-vie-privee.

[71] Sur cette question, en particulier, P. DE FILIPPI et M. REYMOND, « La Blockchain : comment réguler sans autorité », *op. cit.*, pp. 81-96.

consacré par l'arrêt *Google Spain*[72] dans un premier temps et repris ensuite par l'article 17 du RGPD[73]. Le fonctionnement même de la blockchain, qui nécessite de garder trace dans les registres distribués de l'historique de toutes les transactions validées dans les blocs est incompatible avec la possibilité d'une rectification et d'un effacement[74]. Toute rectification ou tout blocage d'accès rendrait totalement impossible la preuve de l'ensemble des transactions et nuirait ainsi à l'ensemble des utilisateurs de la blockchain[75]. Il semble donc que le fonctionnement de la blockchain exige une exception à ces droits à la rectification et à l'effacement. Cette exception ne paraît pas pouvoir être trouvée dans la liste des exceptions prévues à l'article 17, § 3[76], qui visent des hypothèses différentes, ni dans la renonciation des personnes, même informées, à l'exercice de leur droit à la rétractation et à l'effacement[77]. On doit la trouver, comme l'article 23 le prescrit, dans les mesures législatives consacrant le droit de l'autorité

[72] CJUE, 13 mai 2014, arrêt *Google Spain et Google inc. c. AEPD et Mario Costeja González*, C-131/12.

[73] Selon le RGPD, « la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique : a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ; b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ; c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ; [...] ».

[74] Cette impossibilité d'effacement est aussi par nature contraire au principe de minimisation des données et limitation de la conservation des données, voy. art. 5 RGPD. L'idée est en effet que toute donnée doit être effacée une fois qu'elle n'est plus nécessaire.

[75] « Dans la mesure où la blockchain est inaltérable et résistante à la censure et à la modification de par sa conception et la technologie utilisée, son fonctionnement entre en conflit direct avec le droit à l'oubli », P. DE FILIPPI et M. REYMOND, « La Blockchain : comment réguler sans autorité », *op. cit.*, pp. 81-96.

[76] Ces exceptions, si elles existent en matière d'effacement, n'existent pas en matière de rectification.

[77] Il nous paraît en effet impensable que le droit puisse accepter la renonciation par soi-même à l'exercice d'un droit subjectif qu'il a lui-même créé. À cet égard, *contra*, l'article « Blockchain et vie privée » paru sur le site Blockchain et Droit (disp. sur http://www.droit-blockchain.fr/blockchain-vie-privee) qui affirme : « Si la définition de la blockchain semble incompatible avec le droit à l'effacement, existe-t-il des solutions permettant de remédier à cette situation ? À défaut de modification du GDPR, il nous semble qu'à partir du moment où une personne concernée serait clairement et préalablement informée qu'en cas de participation à une blockchain les conditions d'exercice de son droit à l'effacement sont rendues inapplicables, et que cette renonciation est acceptée, ce droit à l'effacement pourrait devenir indisponible de manière légitime ».

publique à limiter les droits de la personne concernée lorsque l'intérêt supérieur de tiers (y compris de l'initiateur de la blockchain) est en jeu[78]. Si tel était le fondement retenu par les autorités européennes, l'article 23, § 2, du RGPD exige que le texte législatif prévoie des garanties. À tout le moins, devrait y figurer l'obligation d'informer toutes les personnes intéressées par l'utilisation de la blockchain, de cette limitation de ses droits à la rétractation et à l'effacement et sans doute, la condition de ne point faire figurer dans le registre décentralisé certaines données sensibles[79] ou le contenu de transactions permettant une « identifiabilité » facile[80]. D'autres réflexions existent encore à ce sujet, mais elles apparaissent peu réalistes au regard du fonctionnement des blockchains[81]. *A contrario*, nonobstant la réflexion reprise ci-dessus quant au caractère intangible de principe des inscriptions enregistrées sur la blockchain, une blockchain peut être modifiée par le consensus de sa communauté, notamment pour la corriger ou la faire évoluer, comme le démontrent la récente décision de scission du bitcoin en 2017 ou la révision du « *The DAO* » d'Ethereum en 2016. Les communautés pourraient donc décider d'organiser pour des opérations délicates ce droit à l'effacement ou en tout cas d'en réglementer l'accès.

Précisons également que régulièrement la plupart des données à caractère personnel ne sont pas stockées directement dans la blockchain. En effet, il n'est pas toujours le plus optimal de tout stocker dans la blockchain en elle-même. Ainsi, certains systèmes complètent leur « infrastructure

[78] « Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir [...] les droits et libertés d'autrui », voy. art. 23, § 2, RGPD.

[79] Ainsi, le Rapport du Parlement européen précité (note n° 3) suggère que les données sensibles et en tout cas de santé ne puissent apparaître.

[80] « Imaginons une plateforme fictive basée sur la blockchain qui fonctionnerait comme un LinkedIn décentralisé, nourri par les contributions de ses utilisateurs. Cette blockchain serait un registre dans lequel n'importe qui pourrait ajouter des informations au sujet d'une personne en particulier – par exemple, en fournissant des liens vers un contenu déjà disponible sur Internet. Toute personne qui souhaiterait en savoir plus sur un individu pourrait parcourir le contenu accumulé par l'entièreté des utilisateurs. Dans un tel scénario, il va sans dire que le droit à l'oubli pourrait légitimement être invoqué, car ce service permettrait n'importe qui d'accéder à une sorte de profil public de la personne », P. DE FILIPPI et M. REYMOND, « La Blockchain : comment réguler sans autorité », *op. cit.*, pp. 81-96.

[81] Voy. par exemple l'article « Blockchain et vie privée », disp. sur http://www.droit-blockchain.fr/blockchain-vie-privee.

blockchain » avec une base de données hébergée ailleurs (tantôt centralisée, tantôt distribuée pour dissuader les attaques informatiques). Cette base de données contient les informations brutes souvent trop volumineuses pour être directement stockées dans la blockchain. Celle-ci est alors accessible en fonction d'autorisations spécifiques qui sont, quant à elles, « gérées via la blockchain ». La blockchain ne sert donc plus qu'à assurer le transfert de clés d'accès. On conserve ainsi les avantages de la blockchain, tout en évitant de mettre inutilement des données volumineuses dans une infrastructure pas adaptée pour cela. Dans ce cas de figure, certes ce qui est dans la blockchain est quasi impossible à supprimer ou modifier, toutefois rien n'empêche techniquement la modification de la base de données, pour autant que la personne qui souhaite/doit effacer certaines données ait les autorisations pour y accéder. Cette modification pourra en plus être monitorée via l'inscription dans le registre de la blockchain d'un accès et d'une modification de données dans la base de données[82]. Ce type d'architecture est non seulement, dans certains cas, plus efficient, mais il permet, de surcroit, aux acteurs de respecter, de manière plus ou moins complète, le droit à l'effacement et à la rectification[83].

18. Les décisions automatisées liées à la blockchain : la question des smart contracts. Le RGPD contient quelques dispositions à propos d'un risque particulier encouru par les personnes concernées lorsqu'elles sont soumises à une décision purement automatisée[84]. L'article 22.1 du GDPR énonce le principe : « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Cependant, le deuxième paragraphe autorise des décisions automatisées dans trois cas : les nécessités de l'exécution d'un contrat, l'autorisation « légale »[85], le consentement explicite de la personne concernée. Cette autorisation est soumise à la condition, ajoute le troisième paragraphe, que le responsable de traitement mette en œuvre des mesures de sauvegarde en faveur de la personne concernée, en particulier le droit à une intervention humaine

[82] Sur cette thématique, voy. *infra*, Chapitre 4.

[83] Pour un exemple de schéma de ce type d'infrastructure, voy. *infra*, § 26.

[84] Sur la genèse et l'analyse détaillée de ces dispositions, voy. T. Tombal, « Les droits de la personne concernée dans le RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie*, *op. cit.*, pp. 531 et s. ; et la littérature abondante sur les dispositions relatives à l'article 22 citée par M. Finck, « Smart Contracts as a form of solely automated processing under the GDPR », *International Data Privacy Law*, 2019, vol. 9, n° 2, pp. 78 et s.

[85] À ce stade, aucune législation n'a utilisé cette exception.

auprès du responsable de traitement. On ajoute que l'existence d'un traitement automatisé et « la logique sous-jacente » doit faire l'objet d'une information particulière selon les articles 13, 14 et 15 du RGPD[86].

L'existence de « smart contracts »[87] liés à des blockchains, qui déclenchent automatiquement l'exécution de la prestation promise et contenue dans la blockchain (par exemple : le versement d'une somme X par une société d'assurance en cas d'annulation d'un vol aérien) suite à l'« oracle » (dans l'exemple, le message envoyé électroniquement par le service de l'aéroport) oblige à l'analyse de ces dispositions : il s'agit bien en effet de décisions[88] prises automatiquement et sur cette seule base (« *solely* ») au sens du RGPD. Leur validité et les obligations du responsable du traitement en cas d'utilisation d'une telle technique de déclenchement de l'exécution du contrat doivent donc être étudiées. La question de la logique sous-jacente ne pose pas de difficulté particulière dans la mesure où le système automatisé repose sur une application totalement transparente du type « Si le message X émanant de telle source et constatant tel événement Y se produit arrive alors le système déclenche automatiquement l'ordre Z qui est exécuté de la manière décrite comme suit. ». La transparence de la logique suivie dans les smart contracts liés à des blockchains ne pose pas, à notre opinion, de difficulté à la différence de ce qui peut se passer avec des décisions basées sur des systèmes d'intelligence artificielle plus complexes et au fonctionnement moins transparent. Il

[86] Art. 13.2.f) RGPD : « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée », même type de libellé à l'article 14.2.g) et à l'article 15.1.h).

[87] « Le smart contract est un programme informatique dont l'exécution est automatisée, conformément aux instructions logicielles et algorithmiques inscrites dans la chaîne de blocs, et dont la fonction consiste à accomplir, sans intervention humaine, certaines opérations en lien avec l'exécution ou la dissolution d'un contrat, suivant la structure "*if this ... then that*..." », Y. POULLET et H. JACQUEMIN, « Blockchain : une révolution pour le droit ? », *J.T.*, 2018, pp. 801 et s.). Pour une analyse plus complète des « smart contracts », de leur intérêt et de leur qualification juridique, voy. la contribution dans le présent ouvrage de H. JACQUEMIN et A. CASSART, « La blockchain et les smart contracts saisis par le droit belge des obligations ».

[88] L'interprétation du mot « décision » est large et s'étend à toute « mesure » (à effet juridique ou à impact économique significatif) prise automatiquement, voy. ARTICLE 29 WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251rev.01, revised on 6 February 2018. M. FINCK (article précité, p. 82) argumente à la fois sur base de l'origine du libellé de l'article 22 (la première version du texte en 2012 utilisait le mot « *measures* »), sur la nécessité d'interprétation large des termes du RGPD, affirmée maintes fois par la CJUE et, enfin, sur le fait que le recours à la blockchain et au smart contract a fait l'objet d'une décision qui a résulté dans la mise en place précisément de ce mécanisme.

faudra également que la personne concernée soit informée des éventuels risques et conséquences pour la personne concernée liés à l'utilisation de cette technologie[89]. Il demeure important que ces explications soient effectuées dans un langage clair, simple et adapté au public[90].

Par ailleurs, il peut être acquis que l'exception contractuelle prévue par l'article 22.2 joue. Comme le dit la loi italienne récente[91], le « smart contract » désigne « un programme informatique basé sur un système de registre distribué dont l'exécution est légalement obligatoire entre deux ou plusieurs parties en référence aux effets antérieurement convenus par les mêmes parties ». En d'autres termes, le « smart contract » n'est jamais que le moyen d'exécution du contrat qui le prévoit. Certes comme le dit, l'article 22, il importe alors que la soumission à la décision automatisée ait fait l'objet d'un consentement explicite, c'est-à-dire, selon l'interprétation donnée à ce concept par le Groupe de travail article 29[92], « une attestation expresse de son consentement, qui pourrait prendre la forme d'une attestation écrite ou le remplissage de documents dans une forme électronique ou scannée, par utilisation de signatures électroniques ». La possibilité de faire jouer l'exception renvoie à une dernière question longuement analysée par l'article de Finck[93]. L'article 22.3 exige que la personne concernée puisse faire appel à une « intervention humaine ». L'interprétation de cette condition par le Groupe de travail article 29[94] souligne que cette intervention ne peut pas être purement formelle, mais suppose une vraie analyse du bien-fondé de la décision au regard des arguments de la personne concernée y compris des documents que cette dernière pourrait apporter et, surtout, que cette analyse soit opérée par une personne indépendante ayant l'autorité appropriée, en particulier de changer la décision. Ceci dit, le texte de l'article n'oblige pas le responsable du traitement à déclencher la procédure de révision éventuelle avant la décision et avant que les effets n'aient été déclenchés. Ainsi, la procédure prendra place après la décision et au cas où elle aboutirait à la révision, il importera,

[89] Art. 13.2.f) RGPD. Précisons que ces risques ont normalement été identifiés préalablement par le responsable du traitement qui aura probablement dû effectuer une *Privacy Impact Assessment* si le traitement envisagé peut engendrer un risque élevé pour les droits etlibertés de la personne concernée, art. 35 RGPD.

[90] Art. 12.1 RGPD.

[91] Loi sur les technologies de registres distribués et les « smart contracts » entrée en vigueur le 13 février 2019.

[92] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, préc. Sur ces exigences, voy. le Rapport de M. Finck au Parlement européen (précité note n° 3), p. 83.

[93] M. Finck, « Smart Contracts as a form of solely automated processing under the GDPR », *op. cit.*, pp. 87 et s.

[94] Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, préc., p. 17.

comme en cas de demande de rectification ou effacement, que les écritures en sens inverse soient effectuées dans les blocs suivants. Enfin, il est clair que la DAO doit informer les personnes concernées de l'existence de la procédure et au cas où plusieurs acteurs peuvent être qualifiés de responsables, que le responsable en charge de la procédure soit identifié, comme le prévoit l'article 26.1 du RGPD.

19. Droit à l'information et principe de transparence. Le RGPD impose au responsable du traitement de communiquer à la personne concernée une série d'information sur le traitement de données qu'il va effectuer. Cette liste d'information à transmettre est reprise à l'article 13 et 14 du RGPD. Comme nous l'avons déjà dit, ces informations doivent être divulguées dans un langage le plus compréhensible possible, tout en restant complet. Sans revenir sur l'entièreté des informations à communiquer, nous souhaitons attirer l'attention sur différents points nous semblant particulièrement intéressants concernant les blockchains.

Premièrement, l'identité du/des responsable(s) du traitement doit être communiquée, ce qui peut être délicat vu qu'il n'est pas encore clair qui est responsable de ce type de traitement et que ces personnes peuvent changer plus vite dans un environnement blockchain que d'habitude, sans mentionner l'utilisation parfois de pseudonyme qui empêche l'identification des responsables du traitement.

Deuxièmement, il doit être indiqué à la personne concernée, l'existence d'un flux transfrontière de données et certaines informations sur le pays de destination. Nous l'avons déjà expliqué, au regard du caractère imprévisible des personnes impliquées dans le traitement des blocs, cette information est difficile à donner dans la mesure où souvent il est compliqué de déterminer à l'avance où pourraient être transférées ces données et à expliquer cela simplement aux personnes concernées.

Troisièmement, il n'est pas formellement imposé au responsable du traitement d'indiquer à la personne concernée qu'il souhaite recourir à une blockchain. Le RGPD n'impose pas une transparence sur les moyens techniques utilisés, sauf si une prise de décision automatisée est envisagée[95]. Dans ce cas-là, une plus grande transparence est exigée. Ainsi une société qui souhaite mettre en place une blockchain privée, pour remplacer une autre technique de gestion des flux d'information, n'a pas à en informer les personnes concernées par ce traitement[96]. À l'inverse, la mise en place de smart contracts pour automatiser l'allocation (ou le versement ?) de prime d'assurance, dans certaines situations, devra être

[95] Voy. *supra*, § 18.

[96] Rapport de M. FINCK au Parlement européen (précité note n° 3), p. 64.

communiquée à la personne concernée. En effet, qui dit smart contracts, dit bien souvent décision automatisée et son existence entraîne donc, suivant les articles 13 et14 du RGPD, le droit de la personne concernée à être informée du fait que ce type de décision va être implémentée. Ce devoir d'information s'effectuera de manière différente en fonction de la relation qu'entretient le responsable du traitement avec la personne concernée[97]. Il nous semble toutefois préférable de faire preuve dans tous les cas, d'une certaine transparence sur l'emploi par le responsable qui utilise les services de la blockchain dans ses relations avec ses clients ou plutôt pour exécuter son service à la clientèle de ce type de technologie. En effet, même si aucun article du RGPD ne l'impose formellement, le responsable du traitement reste soumis au principe de transparence vis-à-vis des personnes concernées[98].

CHAPITRE 5. La blockchain : un bon outil pour le respect du RGPD et la gestion des données à caractère personnel ?

20. Préambule. De nombreuses entreprises et même certains États réfléchissent à mettre en place des blockchains soit pour répondre à divers problèmes liés à l'architecture actuelle de leur infrastructure de gestion de l'information, soit pour satisfaire à des besoins spécifiques à cette entité. Non seulement la blockchain peut s'avérer une solution à différents problèmes pour une administration ou entreprise, mais elle peut aussi s'avérer utile comme outil d'*accountability* et de *compliance* pour le responsable du traitement et d'« *empowerment* » pour la personne concernée.

[97] S'il a ses coordonnées, l'information doit lui être communiquée directement. À défaut, il doit notamment rendre cette information accessible au public (information sur un site web…), art. 14.5.b) RGPD.

[98] Art. 5.1.a) RGPD.

SECTION 1. – La blockchain comme outils pour le responsable du traitement

21. Un outil d'*accountability*. Chaque responsable du traitement est non seulement tenu d'assurer le respect du RGPD, mais également de pouvoir le prouver[99]. Nous ne revenons pas ici sur les éventuels problèmes que peut poser la mise en place d'une blockchain. Concentrons-nous davantage sur la seconde composante de cette notion d'« *accountability* », l'obligation de pouvoir prouver. S'il y a bien une chose qu'il est facile de faire avec une blockchain, c'est de l'auditer (vérifier tout ce qui a été inscrit dedans). Cela peut donc s'avérer utile dans une optique de *compliance* de créer une blockchain afin de pouvoir retracer aisément tout ce qui a été fait, en créant de la sorte une base de données spécifique et fiable... La blockchain servirait ainsi de journal de « *logs and events* », journal infalsifiable en outre de par la vertu de la technologie. Cela peut servir ainsi à garantir une historicité incontestable des transferts de données effectués vers telles entités externes ou des mesures de communication et d'informations prises en cas de *data breach,* conformément aux prescrits des articles 33 et 34 du RGPD. Ceci peut également servir à automatiser certaines procédures avec d'autres entreprises (sous-traitants, sous-sous-traitants, responsables conjoints...), voire APD, en cas d'implémentation de smart contracts qui provoqueraient automatiquement le déclenchement d'une action dans certains cas, et ce de manière certaine, auditable et transparente. Ces blockchains serviraient donc de « boite noire » qui enregistrerait tout ce qui est fait lors d'un incident, de manière infalsifiable, comme celle utilisée dans les avions. L'utilisation de la blockchain permettrait également d'archiver de manière incontestable différents documents rendus obligatoires par le RGPD et d'assurer un suivi de l'évolution de ces documents dans le temps. On peut penser notamment aux contrats de sous-traitance, aux PIA, aux Binding Corporate Rules, à la Privacy policy... Selon certains, cela pourrait également servir de mécanisme de création de confiance pour les flux transfrontières à destination de pays non adéquats[100].

[99] Art. 24 RGPD.

[100] S. STATER, « Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows », disp. sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987.

SECTION 2. – Blockchain comme outil pour la personne concernée

22. Un outil d'*empowerment*. Les blockchains, outils par excellence de désintermédiation, peuvent aussi servir à faciliter la relation entre une personne concernée et ses propres données à caractère personnel hébergées chez un responsable du traitement. Il est ici question de permettre à la personne concernée de pouvoir, directement et sans passer par le responsable, interagir avec ses données à caractère personnel. Classiquement, pour pouvoir interagir avec ses propres données à caractère personnel, il faut passer par le responsable du traitement qui est le seul à véritablement gérer ce qui est fait des données de la personne concernée. Cette thématique de l'*empowerment* de la personne concernée étant l'un des objectifs principaux du RGPD[101], passons en revue quelques possibilités offertes par la blockchain. On notera que les possibilités décrites aux numéros qui suivent illustrent un degré chaque fois croissant de l'*empowerment* de la personne concernée (du simple accès à des données gérées par des responsables de traitements à la gestion par la personne concernée de ses propres données) et conduisent à reconnaître une responsabilisation croissante de cette dernière vis-à-vis des usages faits de ses propres données.

23. Droit d'accès via une blockchain. Certains modèles d'infrastructure offriraient de nouvelles perspectives d'interaction. La personne concernée pourrait via une solution à base de blockchain exercer directement son droit d'accès, sans attendre de réponse du responsable du traitement. La base de données « clients » du responsable du traitement serait ainsi monitorée et tout serait inscrit dans une blockchain de sorte que la personne concernée pourrait savoir en temps réel, qui a accédé à quelles données et dans quel but. Cela permet à la personne concernée de vérifier par elle-même, non seulement, comment sont utilisées ses données, mais également qu'elles ne sont pas utilisées pour d'autres finalités que celles annoncées. Pourrait également être directement accessible pour la personne, le fait qu'un éventuel transfert de données à destination

[101] À ce sujet, nous renvoyons au récent rapport d'évaluation du RGPD après deux ans d'application de celui-ci qui fait notamment le point sur l'impact du RGPD sur cet « empowerment », voy. Commission Staff Working Document accompanying the document « Communication from the Commission to the European Parliament and the Council : Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation », 24 juin 2020, SWD(2020)115.

d'une partie tierce, voire d'un pays tiers, a été effectué[102]. En ce cas, la personne concernée ne doit plus croire sur parole le responsable du traitement, elle peut vérifier par elle-même. Concrètement, en fonction de ce qui est monitoré, dès qu'un accès, un transfert, une modification des données... est réalisé, la survenance de l'événement est enregistrée dans la blockchain[103].

24. Blockchain comme outils d'« anonymisation ». D'autres chercheurs[104] ont également mis en place une architecture qui permettrait à une personne de bénéficier de certains services nécessitant la collecte de certaines données (des services personnalisés nécessitant par exemple une géolocalisation), tout en restant relativement anonyme. La blockchain servirait ici d'intermédiaire entre la personne demandant le service et le fournisseur de service. Pour faire simple, la personne fait une requête, la requête passe par la blockchain, la blockchain masque l'identité de la personne et fait la requête au service, et enfin le service renvoie la demande à la blockchain, qui se charge alors d'interconnecter la demande de la personne et la réponse du service au moyen de clés associées (schème *infra*). Ainsi, pour utiliser un service de navigation nécessitant naturellement une géolocalisation de la personne, la demande de service personnalisé serait envoyée dans la blockchain, qui masquerait l'identité de la personne et ferait une requête auprès du service de navigation. Cedit service enverrait ensuite la réponse personnalisée à cette blockchain, sans même connaitre qui fait cette demande d'itinéraire. Le service reste de la sorte personnalisé (sur base d'une information GPS unique) tout en restant relativement anonyme.

---

[102] Rapport de M. Finck au Parlement européen (précité note n° 3), p. 98 ; C. Wirth et M. Kolain, « Privacy by BlockChain Design : A Blockchain-Enabled GDPR-Compliant Approach for Handling Personal Data », disp. sur https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf.

[103] Ce type de droit d'accès « direct » s'apparente à ce qui est mis en place en Belgique au sujet du numéro de Registre national. Le citoyen belge peut là aussi savoir directement, via un site web, qui a consulté la base de données du Registre national.

[104] G. Zyskind, O. Nathan et A. Pentland, « Decentralizing Privacy: Using Blockchain to Protect Personal Data », disp. sur https://iapp.org/media/pdf/resource_center/blockchain_decentralizing_privacy.pdf.

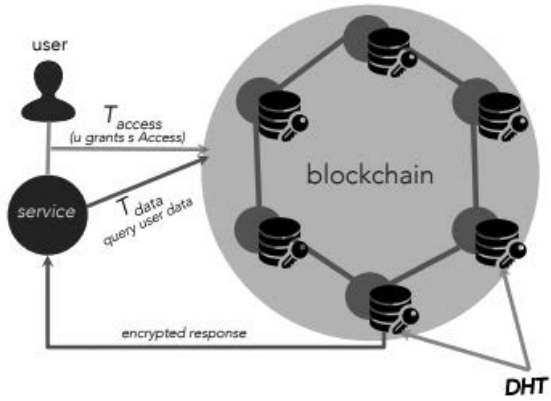

Schéma repris de l'article « Decentralizing Privacy: Using Blockchain to Protect Personal Data »[105]

Dans ce cas-ci la blockchain semble offrir des solutions efficaces permettant d'éviter d'être systématiquement profilé tout en pouvant bénéficier de services personnalisés. Ce type de mécanisme garantirait ainsi un relatif anonymat, en tout cas une mesure de protection supplémentaire pour qui veut quand même bénéficier de certains services qui auraient tendance sans cette solution technologique à être trop intrusifs.

25. Blockchain comme gestionnaire de données personnelles. D'autres encore proposent des infrastructures plus sophistiquées permettant à la personne concernée de créer un « *personal data manager* », un outil basé sur la blockchain qui permettrait à la personne concernée d'encoder dans une base de données personnelle une série d'informations la concernant et d'autoriser elle-même qui peut accéder à quoi et dans quel but, et ce de manière centralisée. Elle pourra également décider de retirer ces autorisations d'accès[106]. Dans ce cas, la base de données qui contient de telles informations personnelles n'est pas hébergée sur la blockchain, mais l'accès à celle-ci s'opère par des clés d'accès disponibles via une blockchain et des smart contracts conformément au schéma repris ci-dessous.

[105] *Idem.*

[106] Certaines sociétés proposent déjà ce type de service. Parmi les plus connues, nous pouvons citer https://datawallet.com/.

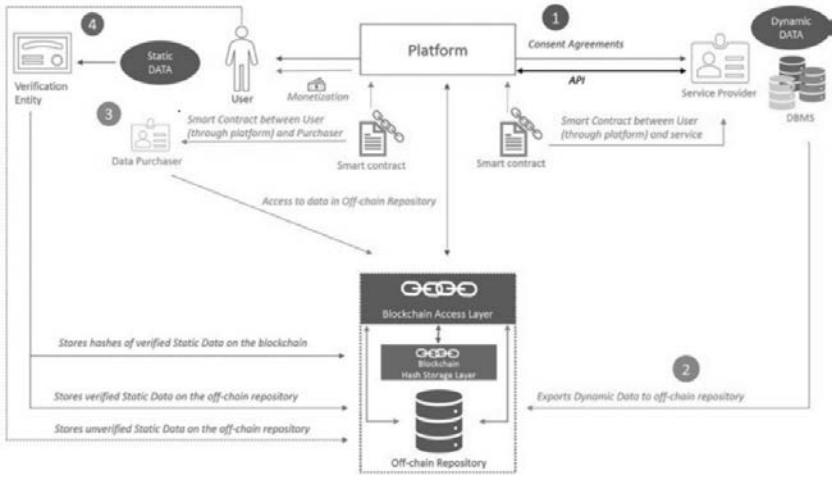

Schéma repris de l'article « BPDIMS : A Blockchain-based Personal Data and Identity Management System »[107]

Ce type d'outils faciliterait grandement la protection des individus. Actuellement, il est impossible pour la personne concernée de gérer et de contrôler efficacement qui utilise quelles données. En outre, une fois l'autorisation d'accéder à certaines informations, ou de collecter certaines informations donnée, il s'avère souvent délicat de retirer cette autorisation. En effet, dans la plupart des traitements de partage de données, ce sont les gros agrégateurs de données (les databrokers) qui créent des profils en récoltant différentes informations disséminées un peu partout sur le web et les vendent à leurs clients. Pour répondre à cette pratique et récupérer « ce qu'il leur serait dû », certains proposent même de pouvoir, via des smart contracts, exiger une rétribution pour chaque donnée partagée[108]. Pour rappel, cette « vente (ou plutôt cession de l'usage) de données » par la personne concernée est explicitement autorisée depuis

[107] B. FABER, G. MICHELET, N. WEIDMANN *et al.*, « BPDIMS : A Blockchain-based Personal Data and Identity Management System; Blockchain-based Personal Health Data Sharing System Using Cloud Storage », *HICSS*, 2019.821, pp. 6855 et s. Le schéma est plus complexe puisqu'il intègre également une possiblité de monétiser l'échange d'information, voy. paragraphe suivant.

[108] *Idem.*

la directive « Digital Content »[109][110]. Toutefois le cadre juridique qui encadre ce type de pratique reste peu clair[111].

Dans une optique moins mercantile, différents projets visent également à faciliter l'échange ou le partage de données à des fins de recherches médicales ou autres...[112]. L'idée est souvent la même : permettre la mise place de *datasets* européen contenant un maximum de données plus ou moins anonymisées[113].

Cela fait plusieurs années qu'on essayait de trouver un outil permettant de rendre plus autonome et souveraine la personne concernée dans gestion de ses données. En effet, il est nécessaire de mettre en place un moyen efficace et centralisé permettant à la personne concernée de contrôler individuellement, ou une fois pour toutes si elle le souhaite, quelles données elle veut partager et dans quels buts. Durant la révision de la directive ePrivacy, il avait notamment été question d'imposer aux navigateurs web de jouer ce rôle de « *Gatekeeper* » pour la gestion des autorisations concernant les cookies[114].

Ce type de plateforme blockchain permet également d'exercer tous les autres droits qui nécessitent un accès direct aux données. En effet, puisque

---

[109] Directive 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, *J.O.*, L136, 22 mai 2019.

[110] La présentation de ce type de services ne signifie pas que nous soyons personnellement favorables au développement de pareilles pratiques consistant à monétiser davantage encore les données à caractère personnel. À ce sujet, voy. Y. Poullet, « La "propriété" des données – balade au "pays des merveilles" à l'heure du "Big Data" », in *Mélanges en l'honneur de Michel Vivant*, Paris, Dalloz, 2020.

[111] Parmi d'autres, L. Dreschler, « Data As Counter-Performance: A New Way Forward or a Step Back for the Fundamental Right of Data Protection? », *Jusletter IT*, 22 février 2018, disp. sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329345; D. Clifford., *The legal limits to the monetisation of online emotions*, thèse défendue en juin 2019 ; EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 mars 2017.

[112] X. Liang *et al.*, « Integrating blockchain for data sharing and collaboration in mobile healthcare applications », disp. sur https://ieeexplore.ieee.org/document/8292361/; Rapport de M. Finck au Parlement européen (précité note n° 3), pp. 91 et s.

[113] Ce partage d'information s'inscrit dans les plans européens de mise en place d'une « *Data sharing economy* » alimentée notamment par des données détenues par des entités privées (« Reverse PSI »), voire des citoyens, voy. Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions: A European strategy for data, COM(2020)66, 19 février 2020.

[114] L'idée a finalement été abandonnée. Pour une étude récente sur la question des cookies voy. A. Delforge, « Le placement de "cookies" sur un site web : la Cour de justice fait le point, l'APD commence à sanctionner », *RDTI*, à paraître.

les données restent gérées par la personne concernée, elle peut elle-même effacer les données qu'elle souhaite ou les corriger...

Si ces outils offrent l'occasion de mieux gérer « son profil numérique », cela n'est pas sans poser certains problèmes « de gestion de son identité » vu l'absence de sensibilisation à ces thématiques[115]. De plus, même si cela permet à la personne concernée de mieux gérer ses données, il faudra également être vigilant à ce que ce type d'outils ne pousse pas tout un chacun à partager avec n'importe qui n'importe lesquelles de ses données.

Conclusions

Certes, le fonctionnement des blockchains ou plutôt de certaines blockchains ne respecte pas totalement les prescrits du RGPD. Certaines rendent difficile la détermination des responsables, la qualification de certains acteurs reste problématique. Si les droits de rectification et d'effacement se révèlent pratiquement impossibles, on relève cependant que des solutions peuvent être trouvées et sont déjà offertes par la pratique actuelle. Par ailleurs, ce fonctionnement soulève des questions délicates d'interprétation du texte européen : à partir de quand glisse-t-on de la pseudonymisation à l'anonymisation ? En matière de flux transfrontières, comment aborder les dispositions relatives à l'application dite « extraterritoriale » du RGPD quand les opérations de minage peuvent s'opérer aux quatre coins du monde que les chaînes de blocs sont hébergées en des milliers d'endroits et contiennent pêle-mêle la trace d'opérations du monde entier ? Comment appliquer la notion de « responsables conjoints » au regard de certains montages qui président à la mise sur pied d'une blockchain. Jusqu'où doit aller l'obligation d'information par un responsable de traitements sur l'utilisation de la technologie de la blockchain ? L'application et la signification de l'article 22 aux « décisions automatisées » que représentent certains smart contracts méritent également notre attention.

Si l'actuelle procédure en révision du RGPD doit être l'occasion de certaines précisions qui permettraient de répondre à toutes ces interrogations et limites révélées par l'analyse présentée, il est clair que nous ne plaidons pas pour une législation spécifique *ad hoc* : « blockchain et

[115] A. Zwitter, O. Gstrein et E. Yap, « Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual », disp. sur https://ssrn.com/abstract=3454513.

protection des données », d'abord parce que la technologie des « *distributed ledgers* » englobe des réalités tellement différentes ; ensuite, parce que la législation envisagée devrait recopier ou au moins renvoyer à la plupart des dispositions du RGPD ; enfin – et nous l'avons montré – parce que la blockchain apparaît, non seulement, comme un moyen sécurisé et fiable aux yeux des tiers y compris des APD pour les entreprises et administrations d'appliquer les prescrits du texte européen, mais, surtout, pour les personnes concernées comme l'outil adéquat pour exercer les droits octroyés par le RGPD voire pour contrôler directement les usages et les destinataires de leurs données. N'est-ce pas là en effet un mérite essentiel de certaines applications de cette technologie de donner au principe dit d'« autonomie », consacré par la jurisprudence du Conseil de l'Europe à travers le concept de *privacy,* sa pleine signification. Comme nous l'avons vu, la blockchain peut être l'instrument d'une maîtrise exercée directement et sans intermédiaire par la personne concernée de ses données et des traitements à leurs propos. Au-delà de ces conclusions, ajoutons deux réflexions. D'abord, notre exposé renvoie souvent aux DAO pour préciser l'application des textes et résoudre, le cas échéant, les incertitudes de cette application. Sans doute, cette solution n'est-elle pas idéale dans la mesure où ces DAO sont souvent ignorées par les personnes concernées ou difficilement compréhensibles. Ne faudrait-il pas que des codes de conduite et des certifications, modes de régulation ou plutôt de co-régulation prévus explicitement par le RGPD (art. 42 et s.) soient proposées et que dans ce cadre, les APD puissent contrôler leur conformité au RGPD et leur réelle effectivité ? Ensuite, seconde réflexion, la mise sur pied de certaines blockchains, en tout cas celles offertes au public en général, mais également certaines privées en raison des risques que leur fonctionnement peut représenter pour les personnes concernées par exemple, de par la nature des opérations y conservées ou de par leur couverture territoriale, etc. doivent conformément à l'article 35 du RGPD être l'objet d'un *Privacy Impact Assessment (PIA)*. Cette tendance à passer d'un contrôle *a posteriori* à un contrôle *a priori* et de confier son déroulement à un groupe multidisciplinaire interne au(x) responsable(s) du traitement ou au concepteur de la blockchain, futur sous-traitant voire au contrôleur externe qu'est l'APD et la publication de cette *PIA* doivent être applaudie. Elle permet de créer pour les personnes concernées une confiance dans un outil technologique dont le rapport *PIA* démontre qu'il est maîtrisé par l'homme.

Ce n'est qu'à ces conditions que le slogan « *Code is Law* » est acceptable.